



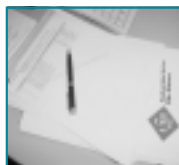
Universitat de les Illes Balears

Piloto de Firma Digital de Actas Académicas

B. Serra, J. Ferrer, M. Canals, J. Ferragut

Centre de Tecnologies de la Informació - Universitat de les Illes Balears
Ctra. de Valldemossa, km. 7,5
07071 Palma de Mallorca, Illes Balears, España
www.uib.es/c-calculo

1 Motivación



- El desarrollo de aplicaciones basadas en firma digital permite **consolidar los servicios** de una **Infraestructura de Clave Pública**.
- Las **limitaciones** que impone la **presencia física** contribuyen a incrementar la **carga** asociada a los **trámites académicos**.
- La firma tradicional de actas es un proceso **sencillo en el planteamiento** pero **complejo en el desarrollo**.
- Las **nuevas tecnologías** en el ámbito de la **identidad digital** abren vías de desarrollo para una **gestión académica** más **rápida** y **eficiente**.

2 Objetivos



- Estudiar los **requerimientos técnicos** y de **organización** para la puesta en funcionamiento de una **Infraestructura de Clave Pública**.
- **Definir, diseñar e implementar** un procedimiento de **firma digital de actas académicas** e **integrarlo** en el actual **aplicativo web** de gestión de actas.
- **Generar conocimiento** a través de la experimentación con **sistemas gestores de certificados digitales**, **aplicaciones de firma digital** y **tarjetas inteligentes**.

3 Arquitectura

- La Infraestructura de Clave Pública del piloto está formada por los siguientes elementos:

Sistema gestor de certificados:

Procesa las solicitudes de los usuarios autorizados y genera automáticamente los correspondientes certificados digitales. Además, gestiona los procedimientos de revocación y publicación.

Directorio LDAP:

Actúa como repositorio de información personal, certificados digitales y listas de certificados revocados (CRLs)

Tarjetas inteligentes:

En una primera fase, su función será la de almacenar de forma segura las claves privadas de los usuarios. En una segunda fase, se experimentará con el uso de criptotarjetas.

- El sistema que permite firmar digitalmente las actas académicas se compone de los siguientes elementos:

Servidor seguro de aplicaciones:

Alberga el aplicativo web de gestión de actas.

Base de datos de información académica:

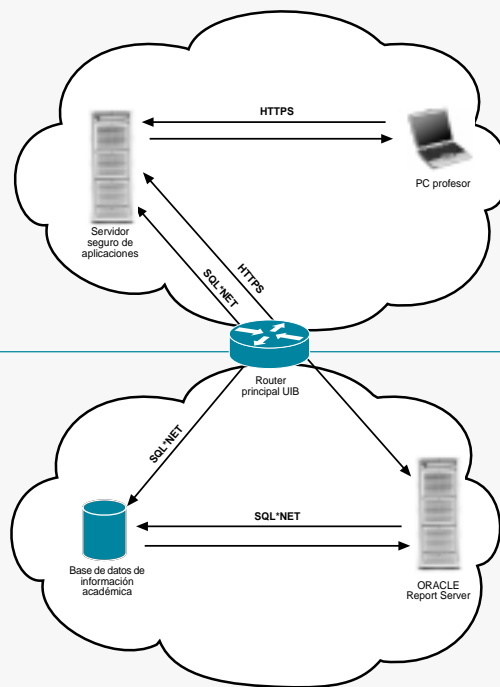
Almacena la información académica de los alumnos y los procedimientos PL/SQL para realizar búsquedas.

ORACLE Report server:

Esta aplicación es capaz de arrancar procesos *report* de ORACLE y dejarlos a la espera de parámetros para que ataquen a la base de datos. A partir de los registros que ésta devuelve genera informes (en nuestro caso, actas) en formato PDF.

Red pública de la UIB

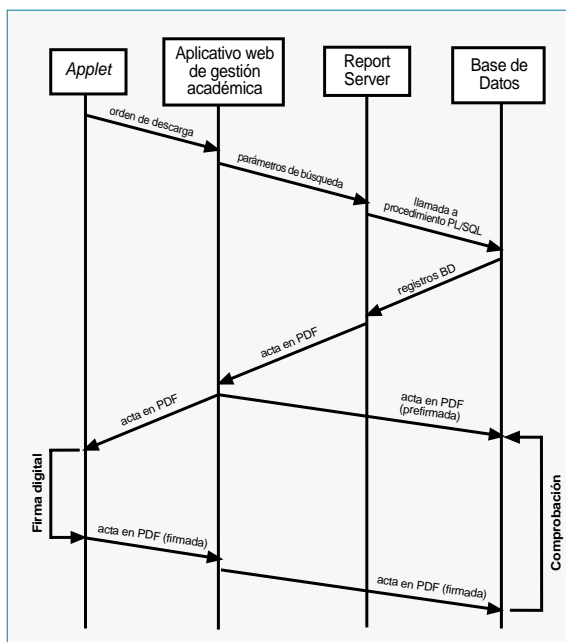
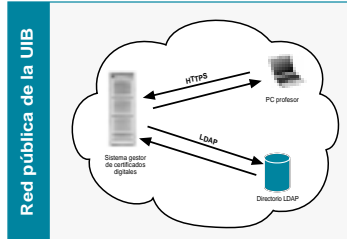
VLAN de gestión



4 Funcionamiento

1.- Registro de usuarios y generación de certificados digitales:

- Los profesores obtienen sus identificadores digitales accediendo vía web a los servicios de una **Autoridad de Certificación Académica**.
- Para filtrar y autorizar las solicitudes, los usuarios deben **autenticarse** contra un **directorio LDAP**. De esta forma sólo se expiden certificados digitales para los profesores participantes en el piloto.
- La **distribución de login/password** para generar los certificados digitales se realiza **presencial y confidencialmente**.
- La **validez** de los certificados digitales es de un **año académico**.



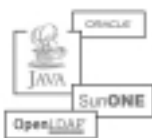
2.- Firma digital de actas académicas:

- El aplicativo web de gestión de actas descarga en el equipo del profesor un **applet Java**. El algoritmo de firma comprende los siguientes pasos:
 - El **applet Java** envía la orden de descarga al **aplicativo web**
 - El **aplicativo web** envía los parámetros al **Report Server**
 - El **Report Server** llama a un procedimiento PL/SQL de la **BD**
 - La **base de datos** devuelve los registros al **Report Server**
 - El **Report Server** genera el PDF y lo envía al **aplicativo web**
 - El **aplicativo web** entrega el PDF al **applet Java** y a la **BD**
 - El **applet Java** firma digitalmente el PDF
 - El **applet Java** envía el fichero PDF firmado a:
 - a) Profesor (*comprobante de firma*)
 - b) Base de datos (*acta oficial*)

3.- Validación de firmas y consistencia de la información:

- Un **proceso interno** de la **BD** **comprueba** que la **firma** del profesor sobre el acta académica es **válida**.
- Para garantizar la **consistencia de la información**, este mismo proceso comprueba que el **contenido** de las dos actas (*prefirmada y firmada*) es el **mismo**.
- En caso afirmativo, **profesor** y **Secretaría Académica** reciben un **acuse de recibo** confirmando que el procedimiento de firma digital concluyó con éxito.

5 Tecnología



- Para la **Infraestructura de Clave Pública** se ha escogido la **suite SunONE Certificate Server**, que incluye:
 - **iPlanet Certificate Management System**, sistema gestor de certificados digitales.
 - **iPlanet Directory Server**, que implementa el directorio LDAP (actualmente se están realizando pruebas con **OpenLDAP**).
- Para la implementación del **módulo de firma digital** se ha optado por desarrollar un **applet** basado en tecnología **Java**.
- La **Base de Datos** de información académica y el **Report Server** están desarrollados con tecnología **ORACLE**.
- El **aplicativo web** de gestión de actas está diseñado en **Java** y **PL/SQL**, aprovechando las funcionalidades de **XML** y **XSLT**.

6 Conclusiones



- Se ha comprobado que existe una **fuerte dependencia** entre los **sistemas gestores de certificados digitales** y los **navegadores web**, lo que **perjudica seriamente** la **interacción** de los profesores con la Autoridad de Certificación Académica.
- La tecnología **Java** es la mejor opción para **garantizar** la **portabilidad** y **evitar** que el proceso de firma digital dependa de las **aplicaciones de navegación y correo electrónico**.
- La firma digital de actas **resuelve las limitaciones** que impone la **presencia física**, pero **genera una nueva problemática** desde el punto de vista de **gestión de documentos** (*modificaciones, diligencias académicas, diligencias administrativas, ...*).
- Paralelamente a los esfuerzos técnicos, es fundamental **transmitir la confianza** necesaria para **garantizar** el éxito del sistema en un **entorno de usuarios no formados** en el ámbito de la identidad digital.